AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

UNITED STATES OF AMERICA
Plaintiff

v.

PEARL HINE NAPPER

Defendant.

Case No. 2:25-MJ-00572-DUTY

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date of February 6, 2025 in the County of Los Angeles in the Central District of California, the defendant violated:

Code Section	*Offense Description*
21 U.S.C. § 841 (a)(1)	Possession with Intent to Distribute Cocaine

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/
Complainant's signature

Andrew Williams, SA HSI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: February 7, 2025

Judge's signature

City and state: Los Angeles, California

Hon. Pedro V. Castillo, U.S. Magistrate Judge
Printed name and title

AUSA: Clifford D. Mpare (x4962)

ATTACHMENT A

PROPERTY TO BE SEARCHED

The following digital device (the "SUBJECT DEVICE"), which was seized from NAPPER on or about February 7, 2025, and is currently in the custody of Homeland Security Investigations in El Segundo, California: An Apple iPhone seized from Pearl NAPPER's belongings.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute controlled substances), 21 U.S.C. § 953(a) (unlawful exportation of controlled substances), 21 U.S.C. § 960 (knowing exportation of a controlled substance), 18 U.S.C. § 554 (knowing exportation of any merchandise contrary to any law), and 21 U.S.C. § 846 (conspiracy and attempt to distribute controlled substances) (the "Subject Offenses"), namely:

a. Records, documents, programs, applications and materials, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

b. Records, documents, programs, applications or materials, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violations;

c. Records, documents, programs, applications or materials, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;

d. Records, documents, programs, applications, materials, or conversations relating to the trafficking of drugs, including ledgers, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs were bought, sold, or otherwise distributed;

e. Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or distribution of drugs or the collection or transfer of proceeds of the above-described offenses;

f. Contents of any calendar or date book, which relate to the above named Subject Offenses or occurring after January 1, 2025;

g. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations, which relate to the above named Subject Offense or occurring after January 1, 2025; and

2. Any SUBJECT DEVICE which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

3. With respect to any SUBJECT DEVICE containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries,

configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment of other devices;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the times the device was used;

f. passwords, encryption keys, and other access devices that may be necessary to access the device;

g. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

h. records of or information about Internet Protocol addresses used by the device;

i. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

II. SEARCH PROCEDURE FOR THE SUBJECT DEVICE

5. In searching the SUBJECT DEVICE (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any SUBJECT DEVICE capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search each SUBJECT DEVICE where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the SUBJECT DEVICE as soon as is practicable but not to exceed 120 days from the date of issuance of the warrant. The government will not search the digital device(s) beyond this 120-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each SUBJECT DEVICE capable of containing any of the items to be seized to the search protocols to determine whether the SUBJECT DEVICE and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

e. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

f. If the search determines that a SUBJECT DEVICE does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the SUBJECT DEVICE and delete or destroy all forensic copies thereof.

g. If the search determines that a SUBJECT DEVICE does contain data falling within the list of items to be seized,

the government may make and retain copies of such data and may access such data at any time.

h. If the search determines that the SUBJECT DEVICE is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain a SUBJECT DEVICE if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

j. After the completion of the search of the SUBJECT DEVICE, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

6. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the

custody and control of attorneys for the government and their support staff for their independent review.

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, Andrew Williams, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint against Pearl Hine NAPPER for violating 21 U.S.C. § 841(a)(1): Possession with Intent to Distribute Cocaine.

2. This affidavit is also made in support of an application for a warrant to search the following cellphone (the "SUBJECT DEVICE"), in the custody of Homeland Security Investigations ("HSI") in El Segundo, California, as described more fully in attachment A: An Apple iPhone seized from NAPPER's belongings.

3. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute controlled substances), 21 U.S.C. § 953(a) (unlawful exportation of controlled substances), 21 U.S.C. § 960 (knowing exportation of a controlled substance), 18 U.S.C. § 554 (knowing exportation of any merchandise contrary to any law), and 21 U.S.C. § 846 (conspiracy and attempt to distribute controlled substances) (the "Subject Offenses"), as described more fully in Attachment B. Attachments A and B are incorporated herein by reference.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there

is sufficient probable cause for the requested complaint and search warrant and does not purport to set forth all my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. BACKGROUND OF THE AFFIANT

5. I am a Special Agent ("SA") with Homeland Security Investigations ("HSI"), an investigative agency within the U.S. Department of Homeland Security, and have been so employed since March of 2023. I am currently assigned to the HSI Office of the Assistant Special Agent in Charge, Los Angeles International Airport ("LAX"), which is responsible for investigating federal crimes involving the illegal importation and possession of firearms and narcotics trafficking, among others.

6. In conjunction with my duties as an SA, I have completed both the Criminal Investigator Training Program and the HSI Special Agent Training Program through the Federal Law Enforcement Training Center in Glynco, Georgia. Prior to my tenure as an SA, I was employed as an officer on active duty in the United States Air Force for approximately six and a half years. While on active duty, I served as a Security Forces Officer, where I conducted and supervised law enforcement and criminal investigative operations on numerous military installations, both within the United States and abroad.

7. Throughout the course of my former and present employment I have received extensive training and experience in

employing investigative means and methods, collecting evidence, interviewing suspects and witnesses, and apprehending violators of law. Additionally, I have training and experience in narcotics identification and investigation, the methods used to distribute narcotics, federal laws related to narcotics and smuggling offenses, as well as practices commonly used to conceal narcotics and communications related to narcotics trafficking to avoid law enforcement detection.

III. SUMMARY OF PROBABLE CAUSE

8. On or about February 6, 2025, NAPPER attempted to travel from Los Angeles International Airport (LAX) to Auckland, New Zealand, on Delta Airlines Flight DL 65, which was scheduled to depart LAX at approximately 10:40 p.m. NAPPER checked one purple hard sided suitcase onto the flight.

9. During a secondary inspection of NAPPER's checked suitcase, United States Customs and Border Protection ("CBP") LAX Officers identified anomalies. CBP Officers conducted a further search of the suitcase and found approximately 14 sealed black plastic bags containing a white powdery substance. The white powdery substance was later tested using the Thermo Scientific Gemini Analyzer, which yielded a positive result for cocaine hydrochloride. The suspected cocaine weighed a total of approximately 23.9 kilograms.

10. When questioned about the suitcase, NAPPER stated to CBP Officers that the suitcase belonged to her.

11. At the time of her encounter by CBP, NAPPER possessed the SUBJECT DEVICE and admitted the device belonged to her. Law

enforcement agents conducted a consensual search of the SUBJECT DEVICE and observed messages regarding her transportation of the suitcase.

IV. STATEMENT OF PROBABLE CAUSE

Based on my involvement in this investigation, my conversations with other law enforcement officials involved in this investigation, and my review of reports and records connected to this investigation, I am aware of the following:

A. NAPPER Possessed Approximately 23.9 Kilograms of Suspected Cocaine Inside Her Checked Luggage.

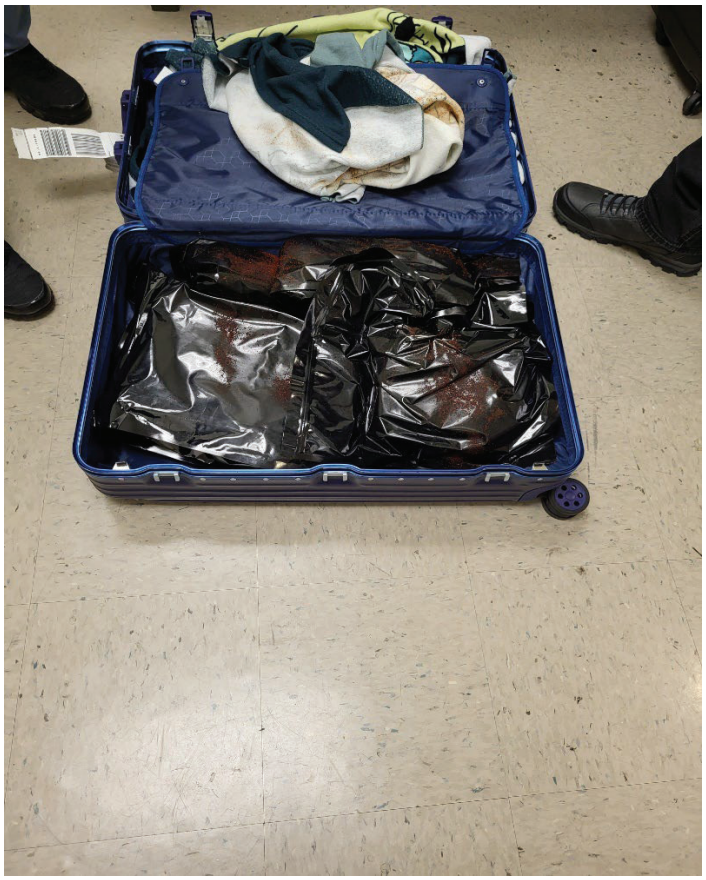
12. On February 6, 2025, CBP LAX discovered approximately 23.9 kilograms of presumptive cocaine inside the checked luggage of passenger Pearl Hine NAPPER. According to CBP, NAPPER was scheduled to fly to Auckland, New Zealand on Delta Airlines Flight DL 65 on February 6, 2025, at approximately 10:40 p.m. NAPPER checked one purple hard sided suitcase onto the flight.

13. According to CBP, NAPPER was selected for an outbound enforcement examination as part of CBP's international flight screening protocols, which are based in part on current international narcotics smuggling trends out of Los Angeles.

14. CBP conducted an outbound inspection of NAPPER's checked luggage, which consisted of one purple hard sided suitcase that bore a bag tag matching NAPPER's name. During a physical examination of NAPPER's suitcase, CBP found approximately 14 sealed black plastic bags containing a white powdery substance. The substance was tested using the Thermo

Scientific Gemini Analyzer.[1] The test yielded a positive result for cocaine hydrochloride. The 14 bags weighed a total of approximately 23.9 kilograms.

15. Images depicting the sealed black plastic bags found in NAPPER's suitcase are attached below:



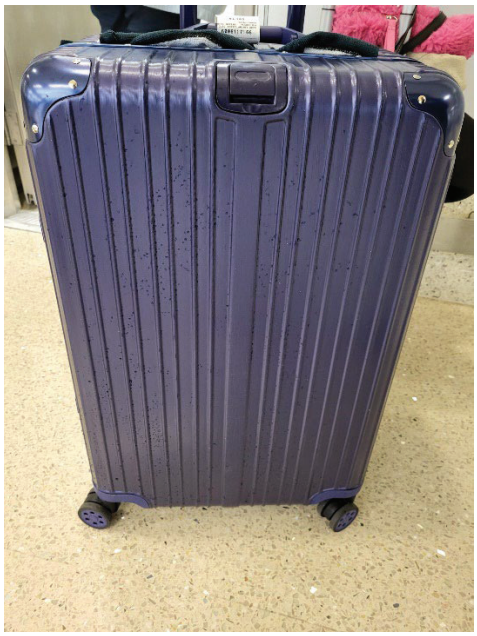
16. On February 6, 2025, I arrived at the CBP Secondary Examination Area in the Tom Bradley International Terminal (TBIT) at LAX. I was informed that NAPPER was detained in a holding room by CBP. Upon arrival CBP informed me that CBP

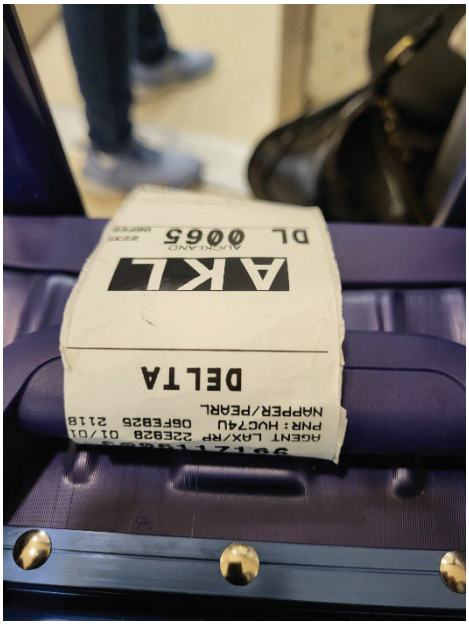
[1] Based on my training and experience, I know that the Thermo Scientific Gemini Analyzer is a machine that allows one to scan drugs through a container and is capable of identifying the type of narcotic being tested.

encountered NAPPER at gate 30A and asked NAPPER for her passport and the purpose of her trip. NAPPER stated she was in the U.S. for a week vacation, staying in Koreatown, and that she had one checked bag. CBP subsequently transported NAPPER to the CBP Secondary Examination Area in TBIT for further inspection.

17. Once in the CBP Secondary Examination Area in TBIT, NAPPER was placed in a search room to review the information she previously told CBP, and NAPPER provided CBP with a bag tag that she confirmed matched the purple hard sided suitcase bearing a bag tag containing her information.

18. Images depicting the Delta Baggage Tag bearing the name Pearl NAPPER as well as NAPPER's checked suitcase are attached below:





B. NAPPER Admits She Knew Her Luggage Contained Concealed Substances.

19. On February 7, 2025, at approximately 1:03 a.m., HSI LAX Special Agents Steve Yoon, Paul Welch, and I interviewed NAPPER in an office located inside the CBP Secondary Inspection Area at LAX.

20. I began the interview by asking NAPPER about her biographical data and advising NAPPER of her rights per Miranda by reading from an HSI Statement of Rights form. NAPPER waived her rights and agreed to speak with law enforcement without a lawyer present.

21. During her interview, NAPPER indicated she was offered $10,000.00 to make a trip from New Zealand to Los Angeles to transport the suitcase in question. According to NAPPER, a female acquaintance approached NAPPER via the Instagram app regarding travel to the United States. From their conversations, NAPPER was of the understanding that the female acquaintance had recently made a similar trip from New Zealand to Los Angeles.

22. After NAPPER agreed to transport the suitcase, the female acquaintance introduced her to a male individual via the messaging app Signal. The two individuals instructed NAPPER to make travel arrangements and, on two occasions prior to NAPPER's travel, NAPPER was directed to park at a specific location in Auckland to receive cash. NAPPER used these funds to book travel arrangements and accommodations for her travel.

23. Also during the interview, NAPPER made statements indicating that, prior to her travel to Los Angeles, she was

informed that the suitcase in question would contain tobacco and/or tetrahydrocannabinol (THC) products and that the suitcase would be washed out with vinegar, presumably to avoid detection by law enforcement.

C. NAPPER Messaged Her Co-Conspirators About Transporting the Suitcase Using The SUBJECT DEVICE.

24. During her Mirandized interview, NAPPER consented verbally and in writing to a search of the SUBJECT DEVICE. NAPPER also provided the passcode to the SUBJECT DEVICE.

25. I visually and manually searched the SUBJECT DEVICE and NAPPER showed me screenshots and messages contained on the SUBJECT DEVICE between NAPPER and the two aforementioned co-conspirators. Based on my review of the SUBJECT DEVICE, there appeared to be a Signal messages between NAPPER and her co-conspirators regarding NAPPER's involvement in the scheme, as well as screen shots of Instagram conversations between NAPPER and the female acquaintance.

26. The interview of NAPPER was terminated at approximately 2:07 a.m.

D. NAPPER Possessed the SUBJECT DEVICE

27. NAPPER possessed the SUBJECT DEVICE on her person at the time of her encounter by CBP.

V. TRAINING AND EXPERIENCE ON DRUG OFFENSES

28. Based on my training and experience and familiarity with investigations into drug trafficking conducted by other law enforcement agents, I know the following:

a. Drug trafficking is a business that involves numerous co-conspirators, from lower-level dealers to higher-level suppliers, as well as associates, to process, package, and deliver the drugs and launder the drug proceeds. Drug traffickers often travel by car, bus, train, or airplane, both domestically and to foreign countries, in connection with their illegal activities to meet with co-conspirators, conduct drug transactions, and transport drugs or drug proceeds.

b. Drug traffickers often maintain books, receipts, notes, ledgers, bank records, and other records relating to the manufacture, transportation, ordering, sale and distribution of illegal drugs. The aforementioned records are often maintained where drug traffickers have ready access to them, such as on their cell phones and other digital devices.

c. Communications between people buying and selling drugs take place by telephone calls and messages, such as e-mail, text messages, and social media messaging applications, sent to and from cell phones and other digital devices. This includes sending photos or videos of the drugs between the seller and the buyer, the negotiation of price, and discussion of whether or not participants will bring weapons to a deal. In addition, it is common for people engaged in drug trafficking to have photos and videos on their cell phones of drugs they or others working with them possess, as they frequently send these photos to each other and others to boast about the drugs or facilitate drug sales.

d. Drug traffickers often keep the names, addresses, and telephone numbers of their drug trafficking associates on their digital devices. Drug traffickers often keep records of meetings with associates, customers, and suppliers on their digital devices, including in the form of calendar entries and location data.

e. Drug traffickers often maintain on hand large amounts of United States currency to maintain and finance their ongoing drug trafficking businesses, which operate on a cash basis.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[2]

31. As used herein, the term "digital device" includes the SUBJECT DEVICE.

32. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally,

[2] As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

33. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it can take a substantial period of time to search a digital device for many reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

34. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VII. CONCLUSION

29. For all of the reasons described above, I submit that there is probable cause to believe that NAPPER has committed violations of 21 U.S.C. §§ 841(a)(1): Possession with Intent to Distribute Cocaine. I further submit that there is probable cause to believe that the items listed in Attachment B, which constitute evidence, fruits, and instrumentalities of violations of the Subject Offenses, will be found in and on the SUBJECT DEVICE, as described in Attachment A.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 7th day of February, 2025.

HON. PEDRO V. CASTILLO
UNITED STATES MAGISTRATE JUDGE